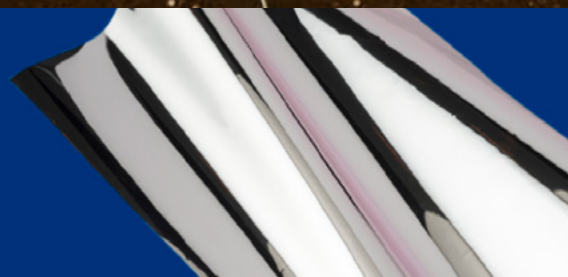
Next Generation Space Defense

MILSATMAGAZINE

September 2024

Cover image is courtesy of Aerospace Corporation



Publishing Operations & Issue Contributors

Silvano Payne
Publisher + Author

Simon Payne
Vice President

Hartley G. Lesser
Editorial Director + Author

Pattie Lesser
Executive Editor + Author

Donald McGee
Production Manager

Teresa Sanderson
Operations Director

Sean Payne
Business Development Mgr.

Dan Makinster
Technical Advisor

Curt Blake
Senior Columnist

Chris Forrester
Senior Columnist

Karl Fuchs
Senior Columnist

Rick Lober
Senior Columnist

Contributors

Lisa Sodders

Amy Walker

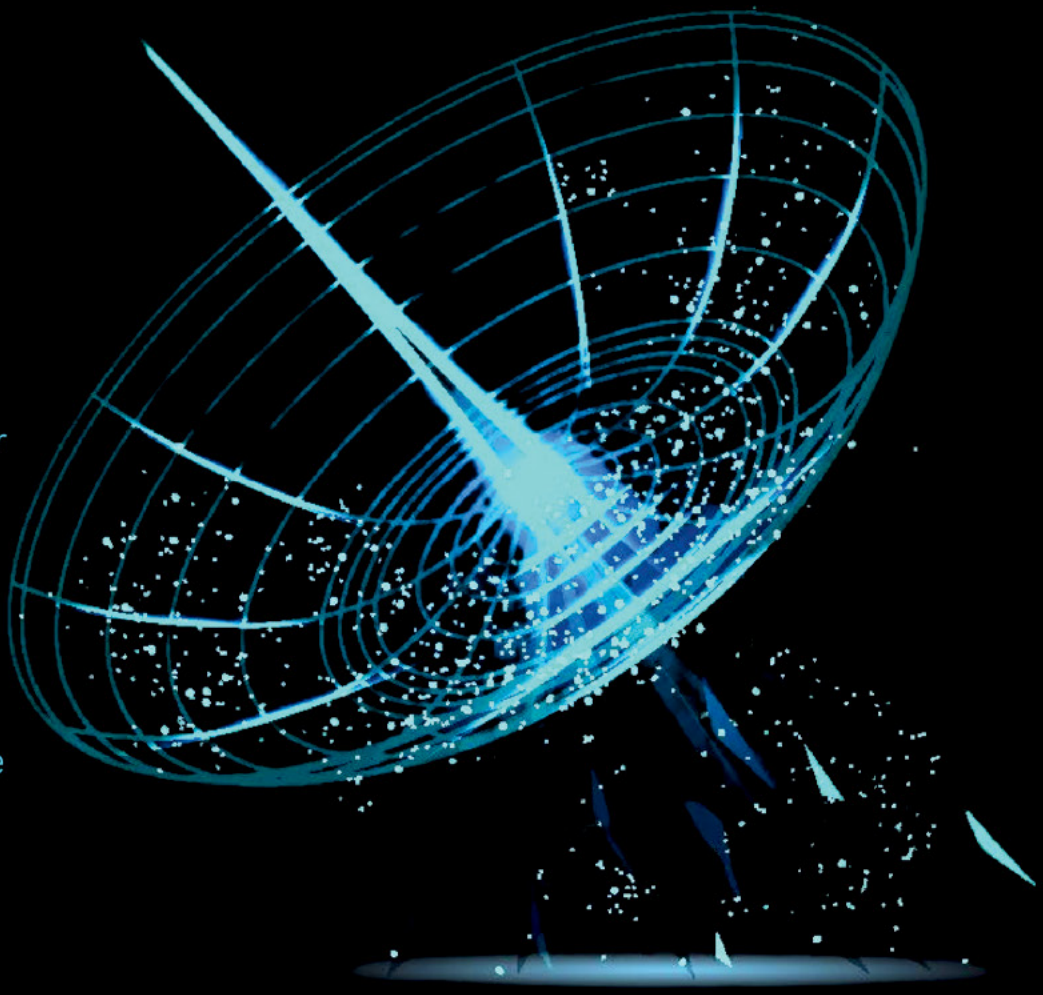
Issue Contents

Advertisers

MilsatMagazine is published 11 times per year by SatNews Publishers, 800 Siesta Way, Sonoma, California - 94576 - USA — Phone: (707) 939-9306 / Fax: (707) 939-9235

Solid-State Power Amplifiers for Satellite Telemetry, Tracking and Control

Take Control - with Tracker Series S-Band and L/S-Band SSPAs from Advantech Wireless Technologies



- 80W to 4kW+
- 1.6 to 2.4 GHz
- Rackmount and Outdoor
- Single-thread, Phase-Combined, 1:1 & 1:2 or Soft-Fail Redundancy
- Ethernet, Webpage and Serial comms port
- GaN and LDMOS Device Structures
- Fitted with High-Power Isolators & Reverse Power Detectors

Advantech has a decades-long history of providing S-Band Solid State Power Amplifiers to Government and Commercial Satcom Operators worldwide.

ADVANTECH WIRELESS
A Baylin Technologies Company

Advantech wireless Technologies

— SPACE SYSTEMS COMMAND BRIEFING —

SPACE THREATS: FROM SCIENCE FICTION TO SCIENCE FACT

Author: Lisa Sodders, Space Systems Command

AS THE U.S. SPACE FORCE CELEBRATES ITS 5TH ANNIVERSARY, SPACE SYSTEMS COMMAND STANDS READY TO PROTECT THE NATION'S SPACE ASSETS

iDIRECT Government

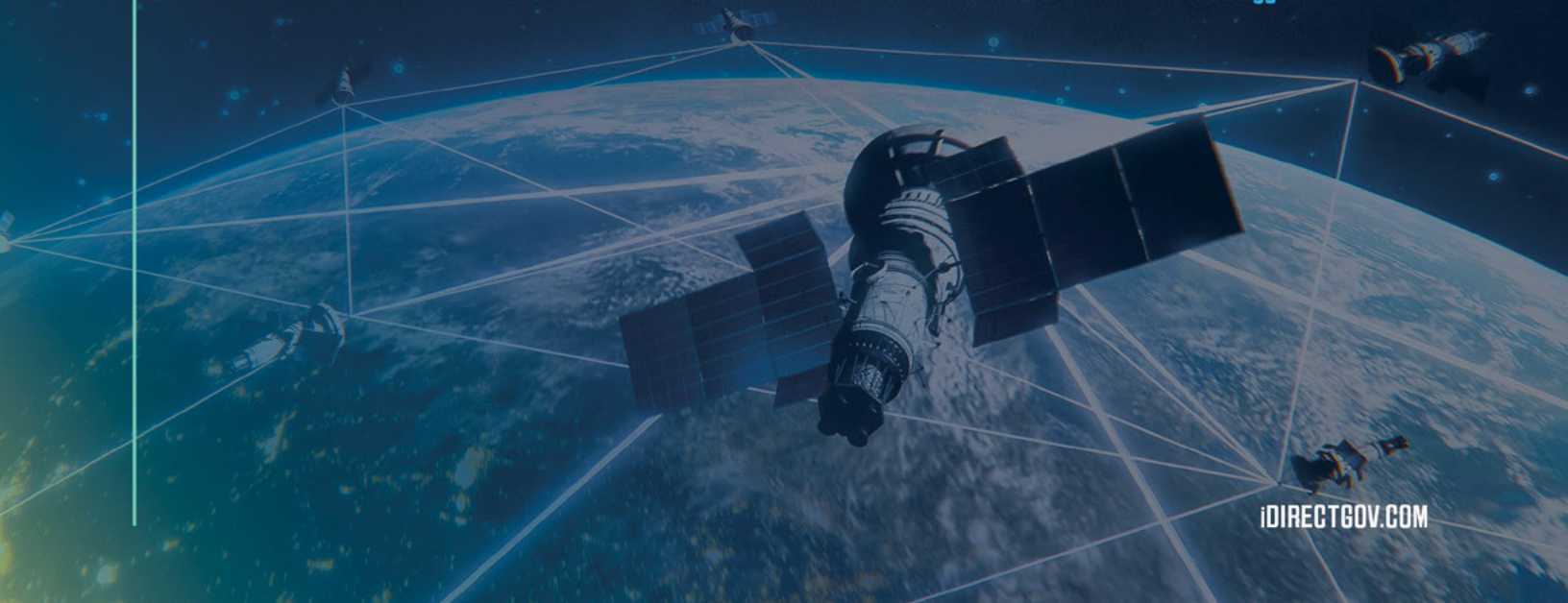
YOUR STRONGEST ALLY IN THE ELECTRONIC WARFARE BATTLESPACE

When SATCOM resiliency, security, innovation and efficiency are paramount to winning the battle — connect with iDirectGov.

At iDirect Government, we offer robust, integrated solutions in electronic warfare (EW), cyber risk and transmission security (TRANSEC) countermeasures, giving the warfighter the solid advantage in offensive and defensive operations.

Our solutions deliver advanced functionality, innovative features and dependable tactical advantages for use on land, in the air and at sea.

iDirect Government ensures that the United States remains at the forefront of MILSATCOM technology.



iDIRECTGOV.COM

When the United States first began launching satellites more than half a century ago, the main threats to those valuable pieces of hardware were the natural phenomena of the space environment, such as excessive radiation and perhaps a collision with a meteorite.


Dr. Scott C. Theiring

"*The trials and tribulations of how to build space craft was the hard part, not thinking that there could be some sort of destructive force trying to go after it besides the harsh environment*," ***Dr. Scott C. Theiring, Director withn Project West Wing of the Aerospace Corporation***, said. "*The average person doesn't give (satellites) a whole lot of thought," Theiring said. "They have the sense that GPS is based on satellites, but they're not really thinking that there may be some sort of threat to GPS or other systems*."

Today, however, the threat to U.S. space assets is real and growing. Space debris from discarded and defunct space vehicles increases the threat of collision and adversaries have, and continue to develop, weapons to deny, degrade, and even destroy space assets, with effects ranging from temporary to catastrophic and permanent.


Major Neal Carter

"*The Space Force was established because these threats are real and significant*," said ***USSF Major Neal Carter, Deputy Director of Intelligence at SSC***. "*Our job is to go after those threats so that the U.S. and its allies can operate freely in space*."

Carter, a former Marine, vividly remembers using space assets as a warfighter on the ground — from GPS to satellite communications and space-based ISR (***Intelligence, Surveillance and Reconnaissance***) — and even missile warning on one occasion.

"*Desert Storm in 1991 is widely considered the first space war,*" ***Carter*** said. "That's when the U.S. military and coalition forces *started using GPS-guided munitions, and we started to see that all these things that operate in space help us achieve lethal effects on the battlefield. Whether it's GPS, satellite communication, or space-based ISR to operate from a military standpoint, we've essentially been using assets in space since the early '90s, and it's only multiplied since then. The U.S. Navy cannot sail without SATCOM, GPS and ISR. Bombers can't fly and hit their targets without literally everything the Space Force provides. Everything we do benefits the joint force in a meaningful way*."

The ***U.S. Space Force*** (**USSF**) and ***Space Systems Command*** (**SSC**) officials are only too aware of the threats posed and they are mission-focused on measures to protect and defend these space assets.

For example, the USSF is reevaluating its space architectures and moving toward using multiple satellites in proliferated constellations in ***Low Earth Orbit*** (**LEO**) instead of a few large, expensive satellites tha are resident in ***Middle Earth Orbit*** (**MEO**) or ***Geostationary Orbit*** (**GEO**), which require more rocket fuel to place them on-orbit.

If one satellite in a ***proliferated LEO*** (**pLEO**) constellation is damaged or destroyed, it is far easier and less expensive to replace that spacecraft, and the capabilities provided by that satellite constellation may not be compromised as multiple satellites in that constellation remain operational.

The satellites SSC launches into space today are entering orbit with advanced anti-jamming technology on board, and USSF's space domain awareness capabilities are continually monitoring space for everything from missiles to rogue adversary satellites that possess the capacity to harm U.S. satellites.

Satellites can receive instructions from ground stations and beam space data back, but can be vulnerable to space threats including cyber attacks. Illustration by Russ Isler, SSC.

These and similar efforts are driven by a laser focus on emerging threats. The most concerning of these are cyber attacks, electronic warfare, directed energy weapons, kinetic energy weapons, high altitude nuclear detonation, and on-orbit attacks.

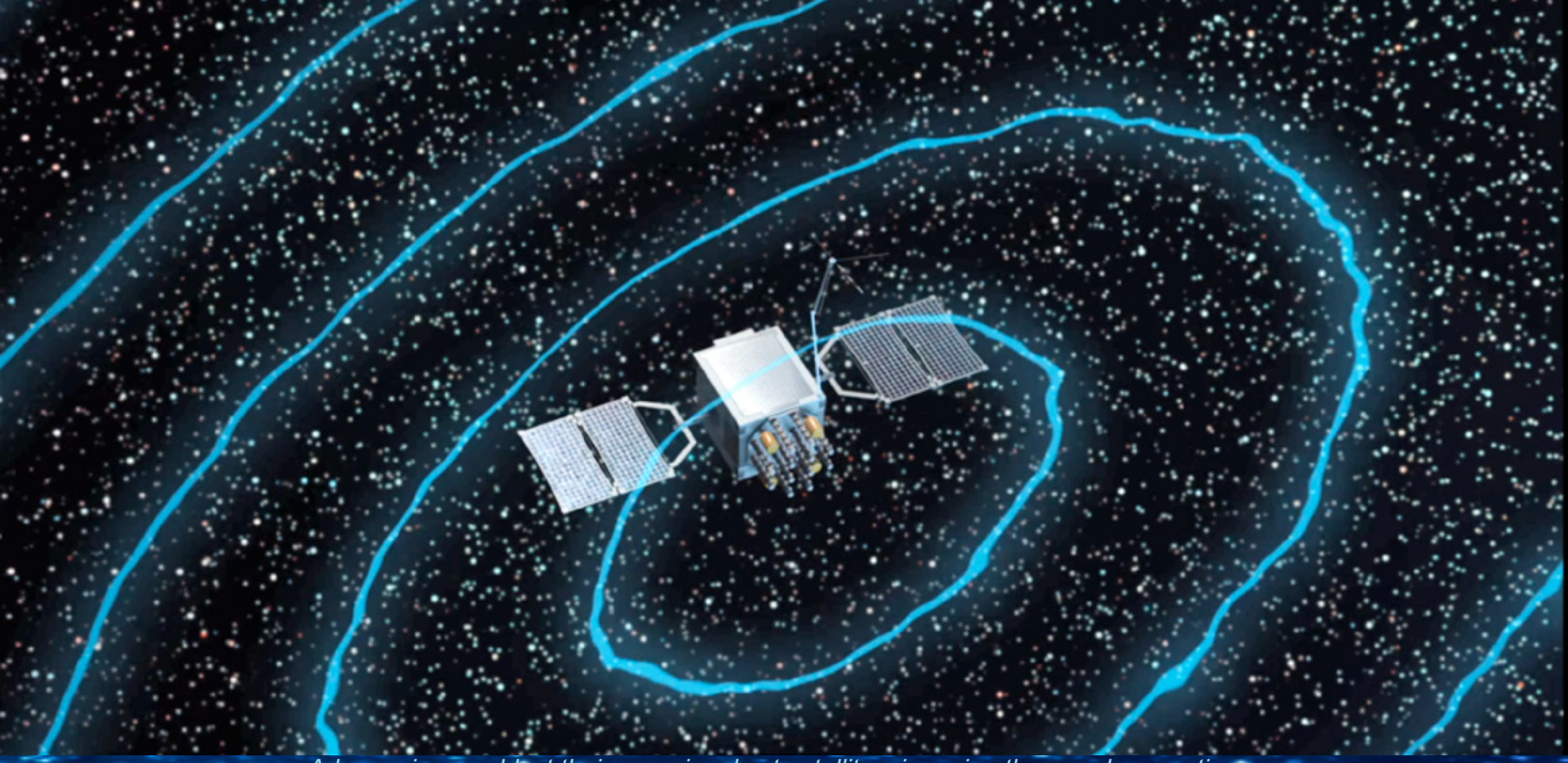
CYBER ATTACKS

A cyber attack can occur when an adversary gains access to a computer system and inserts malicious code. Attacks such as these can include hacking on-orbit satellites; infiltrating the ground-system computers that control and receive data from the satellites; compromising drones; or affecting other computer systems, which, in turn, can compromise everything from satellites to power grids and other crucial infrastructure.

Brian Sessler, chief of SSC's S6 cyber security division, said for ***U.S. Department of Defense*** custom and "***GOTS***" space systems (***Government-Off-The-Shelf***), as opposed to **COTS** (***Commercial-Off-The-Shelf)***, an adversary's attack is less likely to be a direct attack on the satellite itself and more likely to be an initial point of entry attack on and through the ground command and control network.

"*There is the potential for a direct signal to get code injection onto the satellite, but it's going to be much more difficult on a GOTS system because of the rigor that is put into hardening the system*," Sessler said, adding that commercial systems can be less expensive. However, SSC has to vet the supply chain and may have to engage in additional hardening to make the systems more resilient to attack.

"*One of the primary goals of a cyber attack is for reconnaissance*," Sessler said. "*Whether that's for cyber reconnaissance, to further map the system and networks with the goal of maximizing attack effects on the system or just to exfiltrate mission data for intelligence purposes*."



Adversaries can blast their own signals at satellites, jamming them and preventing important space data from getting to the warfighter. Illustration by Russ Isler, SSC.

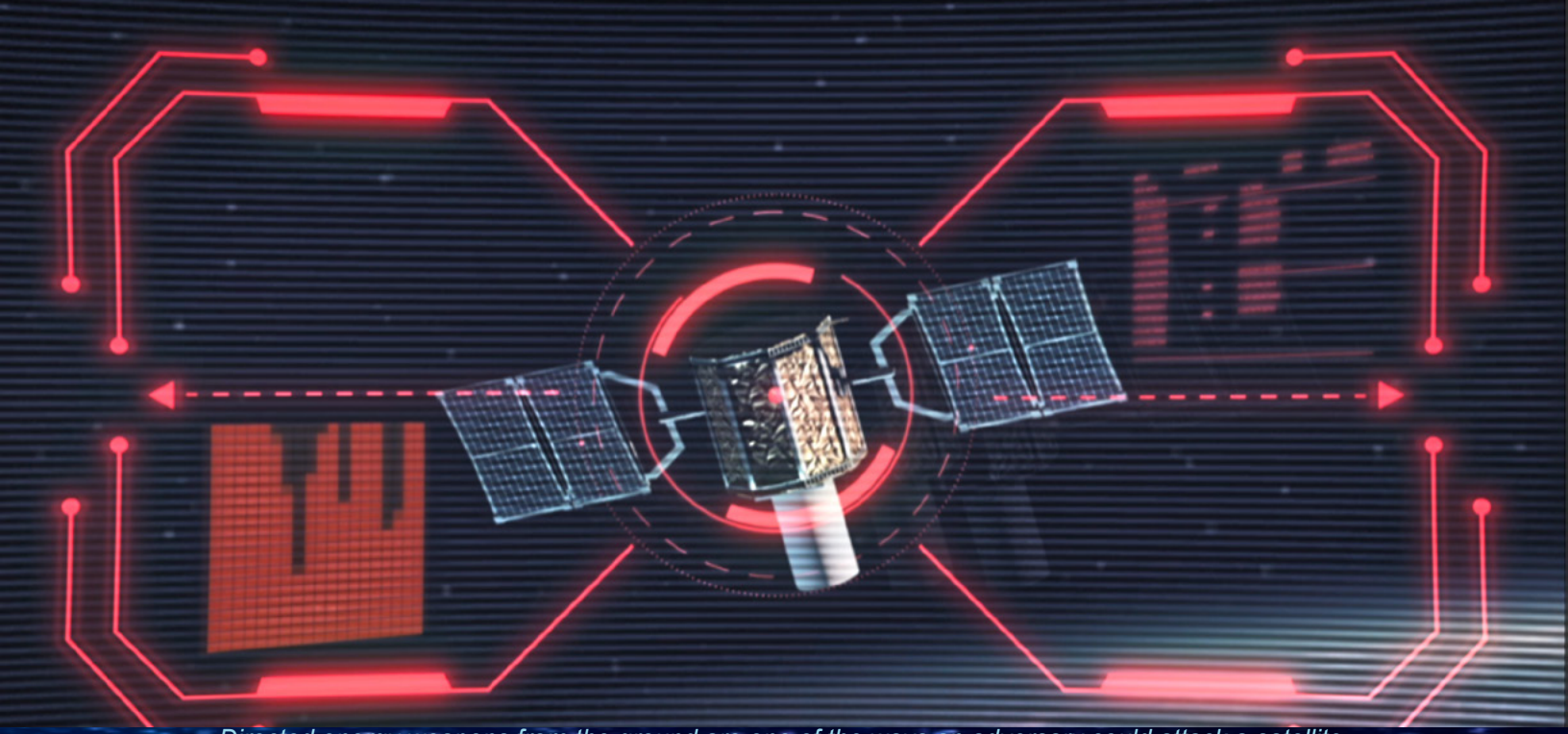
In terms of destruction, most cyberattacks are not causing the computer system to explode or erupt in flames, Sessler said. It's more of a functional kill — impacting the availability of the system or the servers and denying warfighters access to the crucial services those systems provide, such as communications or indications and warning data from a satellite.

"*Our space systems are force multipliers: there are second- and third-order effects if you take out one of our GPS satellites, for example*," Sessler said. "*How many other weapons systems, rely on precision navigation and timing data and services from that satellite constellation? The same can be said for our communications and sensor satellites that are providing critical indications and warning data. Our adversaries are going to want to affect their availability, which is going to affect the kill chain and our ability to execute the mission*."

But it's not just protecting systems once they're operational, Sessler explained. Cyberattack threats apply across all phases of the acquisition process and need to be addressed early.
A lot of it comes down to making sure all personnel are trained and able to recognize phishing attempts, social engineering as well as insider threats that could compromise a system early in the design and development process.

While the areas of vulnerability for a satellite might be different than for a terrestrial system, Theiring said, much of the protective measures are similar: a layered defense, monitoring for unusual traffic, encryption, making sure only certain users are allowed to issue commands under particular conditions, and other measures.

Applying a ***DevSecOps*** process — development, security and operations, a modern approach to software development that integrates security throughout the development process — is essential, Sessler said, as well as constantly conducting penetration testing to make sure systems are hardened against attacks, and making sure individual components aren't corrupted before being integrated with a larger system architecture.



Directed energy weapons from the ground are one of the ways an adversary could attack a satellite. Illustration by Russ Isler, SSC..pdf

What better way to make certain hackers can't attack on-orbit satellites than to launch one and challenge hackers to attack it? ***Hack-A-Sat***, the annual hacking competition sponsored by the ***U.S. Department of the Air Force***, ***SSC***, and the ***Air Force Research Laboratory*** (**AFRL**) invited teams from all over the world to hack an actual, on-orbit cubesat last year — with the goal of being able to use learnings from the competition to help make future satellites more secure.

"*Cybersecurity is very tough because the adversary only needs a pin hole in the attack surface*," Sessler said. "*We're defending against the entire surface, all potential attack vectors, and the adversary only needs to find that one pin hole. Cybersecurity starts early in the life cycle, but at every step of the acquisition process, we need to stay vigilant*."

ELECTRONIC WARFARE (EW)

Satellites can also be vulnerable to electronic warfare in the form of jamming and "*spoofing*" U.S. satellite signals.

"*There are a many different ways an adversary can employ electronic warfare*," Carter said. "*There is ground-based EW, airborne EW, maritime-based EW as well, but what we're seeing more and more is space-based EW. There are also different types of electronic warfare – electronic attack, electronic support and electronic protection*."

Electronic attack is essentially radiating large amounts of electromagnetic energy onto a satellite receiver or a radio antenna, and that makes quite difficult — if not impossible — for (*an operator*) to receive the intended signal.

Carter provided the example and said, "*I have two kids, and they can be very loud. If I'm in the kitchen, washing dishes, and my wife is in the living room and she's trying to tell me something from across the room, but the kids are talking so loudly, it's just impossible for me to hear her — that's jamming*."

"*You're not necessarily doing anything to the intended receiver; you're just making it impossible for that receiver to hear over the noise*," Carter said.

Directed energy weapons from the ground are one of the ways an adversary could attack a satellite. Illustration by Russ Isler, SSC

"*EW has been around for more than 100 years, but as warfare evolves — from the land domain to the air domain to the sea domain — now adversaries can target space assets on-orbit. Satellites communicate with receivers on the ground and adversaires have found ways to, essentially, 'scream' so loudly that the ground receivers can't hear the signal we're trying to send*."

How does the USSF combat this method warfare? By hardening systems and determing procedures by which the receivers are able to ***signal-hop***, Carter said. Another method is to just "*scream louder*" by boosting the power of the intended signal.

"*If an adversary figures out we're communicating on a certain frequency, then they're going to start jamming that frequency*," Carter said. "*So, instead of staying stationary on that frequency, we may configure our radios to frequency-hop, making it difficult for our adversaries to jam us*."

Spoofing is when someone takes a radar signature or other electronic indicator and projects it somewhere else, making the object appear to be in a different location, Carter said. For example, making a ship appear to be in a different location than it actually is, and making it harder for someone to target that object and close the kill chain, that's spoofing.

DIRECTED ENERGY WEAPONS

In a similar vein, directed energy weapons can be used to damage and degrade equipment and signals. Such an attack might take the form of a ground-based directed energy weapon, radiating lasers to blind or dazzle satellite sensors on-orbit — or it could be a directed energy weapon on-orbit, Carter said.

"*Having a ground-based weapon gives the adversary a little more power boost, and they can maintain that system on the ground, but in orbit, you can get a lot closer to the target*," Carter said. "*There are trade-*

offs for both of those, and we expect to see more examples of this in the coming years.

"*If we have an ISR satellite that we're using to observe airfields, ships, missiles, or ground troops – all things that the joint force and the national command authority need to build intelligence assessments – and there's a directed energy weapon with a laser dazzler or other type of emitter that's engaging and cooking that satellite, the sensors on that bird are fried*," Carter said. "*If we can't see our targets on the ground, then we can't get that intel to the warfighter, the commander, or the president. It's a significant threat if adversaries can go from satellite to satellite, pinpointing and targeting our ISR birds.*"

Whether the damage is temporary or permanent depends on exposure time and proximity — and for an on-orbit weapon, how close the adversary can get before the rogue satellite is spotted, and countermeasures are activated, Carter said.

In addition to physically hardening satellites to protect them, another way to safeguard satellites involves making certain they are maneuverable and also ensuring the U.S. and allies have the ability to detect when a satellite is being attacked, Carter said.

"*With material hardening comes other drawbacks and tradeoffs. If you put shielding on your system, you could weigh it down too much, and the more weight you put on a satellite, the more expensive it becomes to launch, maintain, and keep in orbit. There's a lot of considerations we have to account for as we're designing a satellite and before we launch it.*"

KINETIC ENERGY WEAPONS

Kinetic energy weapons are weapons designed to destroy space assets, either by colliding with them or by using warheads to destroy them. Kinetic weapons pose an additional threat in that the fragments of the destroyed satellite then become space debris, thereby posing a threat to other space vehicles.

"*The most visual representation that we can remember is the movie '**Gravity**' (2013),*" Carter said. In that film, Russians destroy one of their defunct satellites, and the resulting space debris field destroys a space shuttle, damages the ISS, and takes out several communications satellites.

Both Russia and China have demonstrated the ability to use ***direct-ascent anti-satellite*** (**ASAT**) weapons. China tested an ASAT weapon in January of 2007, destroying a defunct Chinese weather satellite, and resulting in the creation of a debris field that possessed more than 3,000 pieces of space debris.

ORBITAL DEBRIS CREATED BY ASAT TESTS IN SPACE

DATE	COUNTRY	ASAT SYSTEM	TARGET	INTERCEPT ALTITUDE	TRACKED DEBRIS	DEBRIS STILL ON ORBIT	TOTAL DEBRIS LIFESPAN
Oct. 20, 1968	Russia	IS	Cosmos 248		252	79	50+ years
Oct. 23, 1970	Russia	IS	Cosmos 373		147	35	50+ years
Feb. 25, 1971	Russia	IS	Cosmos 394		118	45	50+ years
Dec. 3, 1971	Russia	IS	Cosmos 459		29	0	3.3 years
Dec. 17, 1976	Russia	IS	Cosmos 880		127	57	45+ years
May 19, 1978	Russia	IS-M	Cosmos 970		73	64	40+ years
Apr. 18, 1980	Russia	IS-M	Cosmos 1171		48	6	40+ years
Jun. 18, 1982	Russia	IS-M	Cosmos 1375		64	60	35+ years
Sept. 13, 1985	U.S.	ASM-135	Solwind	530 km	287	0	18+ years
Sept. 5, 1986	U.S.	Delta 180 PAS	Delta 2 R/B		17	0	< 1 year
Dec. 26, 1994	Russia	Naryad-V?	Unknown		27	24	25+ years
Jan. 11, 2007	China	SC-19	FengYun 1C	880 km	3536	2786	15+ years
Feb. 20, 2008	U.S.	SM-3	USA 193	220 km	175	0	1+ year
Mar. 27, 2019	India	PDV-MK II	Microsat-R	300 km	130	1	3+ years
Aug.-Dec. 2019	Russia	Cosmos 2535	Cosmos 2536		30	16	3+ years
Nov. 15, 2021	Russia	Nudol	Cosmos 1408	470 km	1790	300	Unknown
				Total	**6850**	**3472**	

A graph of orbital debris created by ASAT tests in space, courtesy of the Secure World Foundation, included in the organization's ***SWF Global Counterspace Capabilities Report.***

"*A 2023 report from the National Space Intelligence Center was looking at how many pieces of debris were still in orbit from the 2007 destruction that China executed, and the estimate was there were still 2,700 pieces still in orbit, basically a decade and a half later*," Theiring said. "*So those things are still flying around in space and adding to that environmental threat. And they're not clearing out of that minutely thin atmosphere that high up.*"

Objects in LEO could be travelling as fast as 17,000 mph, so depending on the size of the object and what it hits, space debris can be extremely destructive, Theiring said.

"*If it's the size of a grain of sand, the satellite lives to survive another day, but if it's the size of a baseball, it's probably going to be catastrophic*," Theiring said. "*It depends on what it hits and then it becomes very random – if it hits the solar cells and causes the half-loss of power, maybe half the mission is still working. But if it hits a key component, the satellite is dead, even if it was just a small piece of debris*."

In November of 2021, Russia tested an ASAT and destroyed one of their older satellites, generating more than 1,500 pieces of trackable space debris in LEO and forcing two cosmonauts (*who happened to aboard the International Space Station at the time*) to shelter in emergency vehicles. Even today, the ISS is still occasionally having to maneuver to avoid debris from that 2007 Chinese ASAT test.

"*Being able to set those norms — and not just from a human spaceflight perspective but a space defense and space warfare perspective — is important*," Carter said. "*If nothing else, our job in the Space Force is to prevent conflict as much as it is to win in the event of a conflict. I joined Space Force so my kids don't have to fight the wars I did*."

Space Domain Awareness (**SDA**) — not just knowing where U.S. space vehicles and those of our partners are located, but also those of our adversaries — tracking space debris, and characterizing threats and hazards — is all part of the USSF's decision-making process in threat identification and determining what phenomenon poses a threat and what is benign, Carter said.

HIGH-ALTITUDE NUCLEAR DETONATION

An adversary could also launch a nuclear weapon and detonate it at a high-altitude, creating a radiation burst that could damage or destroy satellites.

An adversary could launch a nuclear weapon and detonate it at a high altitude, creating a radiation burst that could damage or destroy satellites. Illustration by Russ Isler, SSC.

Adversaries do have this capability, and it's not new, Carter said. Both the U.S. and the former Soviet Union developed this capability decades ago, in the 1950s.

"*The higher the nuclear detonation is in altitude, the bigger the problem because of yield*," Carter explained. "*When you have a high altitude or high orbit, the yield that the altitude gives the radiation, and that energy, creates problems for other orbits, not to mention the Earth's protective magnetic belts. It has the potential to wreak havoc on communication satellites and GPS satellites and everything we depend on for our way of life. It's a huge threat*."

Employing this threat/putting this threat into action/acting on this threat would make space inaccessible for not only the United States, but for the adversary as well and "*we'd hope that's a good deterrent against deploying that kind of weapon. But we can't go off hope alone*," Carter said.

In addition to SDA and strong missile detection and tracking systems, "*open lines of communication with our joint partners and international allies -- as well as our adversaries — is important*," Carter said. "Just because we may not be on the best terms wit*h a nation state doesn't mean we shouldn't talk to them to prevent miscalculation and misunderstanding and ultimately, a tragedy*."

ORBITAL ATTACKS

Adversaries have also demonstrated the ability to launch satellites with smaller satellites nested within them as well as satellites with robotic arms. While such capabilities could be used for peaceful purposes — repairing or refueling satellites — this kind of technology also could be used to deploy satellites capable of disabling or destroying other spacecraft.

"*That's the tricky thing about space operations and space warfare in general*," Carter said. "*A lot of what a nation state can launch into orbit can appear benign and peaceful, but that's kind of the cover story.*

Just because an adversary says 'This is for peaceful purposes; this is for repair operations," doesn't mean it's not worth us paying close attention. Does it have the capability of maneuvering near or onto our vehicles and doing some serious damage? That's something we're paying very close attention to.

"At least one Chinese satellite has been identified as having a robotic arm on it, and that satellite moved close to an old Chinese satellite and moved it into a super synchronous (graveyard) orbit," Theiring said. "*The use of robotic arms are required for refueling or for servicing and other peaceful and productive uses. However, the skillsets required for that also overlap with the ones required for more nefarious purposes. In this case, the towing of that satellite was a net benefit – it got rid of a piece of space junk in GEO.*"

Hardening space vehicles, ensuring maneuverability and early detection of threats are all good defensive measures to mitigate the threat, Carter said. However, so, too, is a pLEO constellation where many smaller, less expensive satellites can provide more resilience.

In many respects, space is still a very new frontier. The ***Outer Space Treaty of 1967*** established a framework for space law, but it is proving to be outdated as more nations participate in space and new technologies. Plus, greater numbers of satellites increase the need for coordination and universal rules.

The unique components of orbital mechanics also mean that if an adversary decides to destroy another country's satellite, they could end up jeopardizing more than just one nation's spacecraft. Additionally, there's the sticky problem of attribution: how do countries determine who is responsible for damaging another nation's space vehicle?

"*Attribution is the tricky part about space warfare – such as the strategic implications of a rendezvous-and-proximity operation*," Carter said. "*It's easy for (airplane) pilots to see some sort of incursion: a Russian plane flying in American air space, near Alaska. They can see the markings, they know what type of planes the Russians fly, and the pilots can communicate with and take pictures of their Russian adversaries.*

"*It's a lot harder to do that in orbit – and then convince the international community that it's occurring. And with that, are we burning sources and methods of how we collect the intelligence.*" Carter said.

"*Even as recently as 10 years ago, space wasn't as competitive, congested or contested to the point where we needed a dedicated military service to operate solely in the space domain*," Carter said. '*Now, it couldn't be more important, and our role will only continue to grow. As commercial interests start to expand into every orbit and cislunar space, our job is only going to get harder and become more important.*"

Space Systems Command is the U.S. Space Force field command responsible for acquiring, developing, and delivering resilient capabilities to protect our nation's strategic advantage in, from, and to space. SSC manages a $15.6 billion space acquisition budget for the Department of Defense and works in partnership with joint forces, industry, government agencies, academic and allied organizations to outpace emerging threats. Our actions today are making the world a better space for tomorrow

*For additional information, contact Space Systems Command at **SSC@spaceforce.mil** and/or follow on **LinkedIn**.*

Author Lisa Sodders writes the monthly Space Systems Command column for MilsatMagazine.

High Throughput Tactical FlyAway & Gateway

2.4m Full Hemispherical Tracking Terminal
GEO / MEO / LEO Multi-Orbit
X, Ku & Ka Bands
SATCOM / SIGINT / EW / EO

AvL TECHNOLOGIES
avltech.com

Let's Talk Multi-Orbit
@ MilSat Symposium Booth 12

COMMAND CENTER

TIM WINTER, CHIEF EXECUTIVE OFFICER, IDIRECT GOVERNMENT

Tim Winter

Tim Winter oversees the corporate strategy and leads the iDirectGov team to bring solutions to the military satellite communications (MILSATCOM) arena. He brings more than 20 years of experience in satellite communications.

Prior to joining iDirect Government, Winter served as vice president of global accounts and global government & defense at parent company ST Engineering iDirect. Winter managed all strategic global account engagements and capture pursuits for International Defense opportunities.

Previously, he managed the satellite networks division at L-3 Communications where he led all sales and business development efforts for managed satellite communication, data networks and operational field services.

Winter served in the U.S. Navy and flew P-3 Orion aircraft as a Naval flight officer on active duty for eight years. He continued his service in the United States Navy Reserves, flying P-3 aircraft and the BAMS-D UAV through 2022. He recently retired from the U.S. Navy with the rank of commander.

Tim has a master's degree in business administration from Georgetown University, Washington, DC, and a bachelor of science degree as a Trident Scholar from the United States Naval Academy, Annapolis, Maryland. He is chairman of the board for the Minerallac Company.

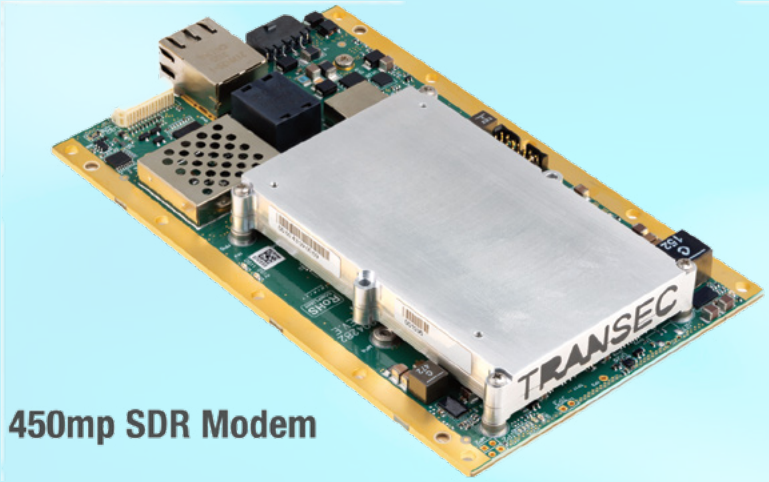
Mr. Winter, more than a year has passed since you took over the top position at iDirectGov. What are your major accomplishments in this timeframe?

TIM WINTER

It's been a great year, and I have been able to build upon iDirect Government's outstanding heritage of serving the warfighter and government customers with secure connectivity anytime and at any location.

To date, we have pushed to create an even more resilient, secure and seamless satellite communications environment. The team continues innovating and creating advanced solutions. Many of these innovations build upon our specialized ***Communication Signal Interference Removal***™ (**CSIR**™) technology, which features crypto-agility, anti-jam and strengthened security for the tactical edge and warfighter.

We debuted the ***REVOLUTION 450mp*** *software defined radio* (**SDR**) modem that extends satellite communications orbit and waveform choices for the warfighter, regardless of their location. Plus, we introduced the new ***Evolution Defense 4.6.1*** software, delivering improved security, strengthened *transmission security* (**TRANSEC**) and augmented CSIR technology.



450mp SDR Modem

We saw a need for better mission readiness with training and we integrated our Tactical Hub with a partner, ***Tampa Microwave*** and its ***Quad Band Satellite Simulator*** (**QBSS**). This provides

an end-to-end system validation, *radio frequency* (**RF**) equipment testing, training, maintenance and pre-deployment exercises of hub and remote terminals in a simulated satellite network of as many as 1,000 remotes within a range of 300 feet.

These accomplishments are the result of a bright and dedicated teams who work to modernize the military and meet the ever-changing needs of our customers in the new space war.

How did your interest develop in satellite communications in general, and, more specifically, in MILSATCOM?

TIM WINTER

First and foremost, I was a user of satellite communications as a Naval aviator. Early in my career, we relied on narrowband MILSATCOM capabilities and networks. Later, I used both narrowband and wideband SATCOM networks. The necessity and capability set provided by SATCOM immediately stoked my interest.

Given your U.S. Navy experience as a Naval aviator and retiring with the rank of Commander, what drew you into the military communications market segment to initiate a new career?

TIM WINTER

It was a bit of an interesting path into the military communications market. Following my time as an active-duty Naval aviator, I joined Northrop Grumman to assist with its advanced ISR future technologies. After a stint there and a few years at business school, I went into the downstream oil and gas industry only to eventually find my way back into the U.S. Department of Defense (DOD) satellite communications market. I was more than happy to be back supporting the greatest customers in the world.

How do you see your U.S. Navy experience assisting you with the executive leadership of iDirect Government?

TIM WINTER

My time in the U.S. Navy greatly influenced my leadership and approach to individuals and organizations. To serve was an honor. Leading such a great group of individuals codified my approach to a servant leadership style. I have tried to bring this style to my leadership roles since leaving the Navy. Like the Navy, I am honored to lead the iDirect Government Team and the incredibly important customers that we serve.

What are the challenges encountered when promoting iDirectGov products to the various military segments to ensure they have the "latest and greatest" tech provided by the company?

TIM WINTER

Not all SATCOM is created equally. Different technologies and different products and solution sets provide unique capabilities. Our goal continues to be a true partner with the end-user and highlight to them where our capabilities fit into their mission needs. We actively promote our products to the mission needs for which they are best fit. Does this mean we can't be everything to everybody? Potentially. But I believe it allows us to be laser focused on the capabilities we can provide — and fulfill our goal of being the best provider of these capabilities.

How do you feel this opportunity will enhance and additionally drive iDirectGov to be considered as one of the trusted, major suppliers to organizations that are involved in national defense, here in the United States and with our Allies?

TIM WINTER

Our goal at iDirectGov is to continually improve our product and service offerings to our customers. At the center of these efforts, are our advanced security features, resiliency and commitment to providing the most secure satellite communication links. Of note, many Allies of the United States operate iDirect-based networks. With the growing importance of coalition operations, this natural fit of interoperability makes iDirect a de facto solution for the U.S. government and our Allies.

How is the government assisting commercial companies, such as iDirectGov, in upgrading and supporting the capabilities of our Armed Forces through the passage of legislation and funding to provide the training and equipment necessary to field the crucial technology required to support warfighters?

TIM WINTER

The provisioning of solutions and sales cycle with the U.S. government can be long. This, obviously, can be counterproductive to the rapidly evolving needs of the end-user. Recently, the DOD has embraced quicker, smaller *Transactional Authorities* that can lead to the expedited development of needed or advanced capabilities. iDirectGov is currently doing work for the ***Defense Innovation Unit*** (**DIU**) which is one of the other Transactional Authorities. We believe in this approach employed by the U.S. DOD and are very pleased to be supporting the DIU in the development of 5G co-interference.

Electronic Warfare (EW) is bringing new security concerns to MILSATCOM. What can be done to combat EW communications threats in the new space war?

TIM WINTER

The new space war, with the rise in EW and jamming of communications networks, is certainly challenging. Malicious actors are always working to jam communications and thwart the efforts of troops on land, in the air and at sea.

To combat EW, countermeasures must be in place in every DOD solution. *Signal excision technology* is among the preferred choices to counter EW threats.

iDirectGov's CSIR™ monitors and eliminates an interfering signal from the authorized signal in real-time, giving the DOD a leg up. And we know, CSIR excision technology effectively mitigates a wide range of interferers, from carrier waves to multiple strong interferers, without requiring prior information on them. It can locate fast-moving and intermittent interference and restore the quality of the original signal, without requiring additional hardware. This combats adversaries who are increasing their implementation of *signal intelligence* (**SIGNET**) to attack military and government spectrum use by jamming.

We know Defense-based networks must work in contested environments before, during and after the shooting starts. Anti-jam technologies, such as signal incision, are bringing secure satellite transmissions and enhanced systems to the ever-increasing mobile battlefield for data, voice, and command and control and other MILSATCOM.

The path forward for secure, interoperable communications in the wake of EW communications threats in the new space war involves CSIR signal excision technology that is effective, reliable, fast, trustworthy and secure.

iDirectGov is building an operational 5G co-channel interference mitigation solution prototype for the DIU. How critical is this development to the military?

TIM WINTER

The DOD needs a connected battlefield without interference, and this contract to build an operational 5G co-channel interference prototype suits the specialized needs of the military.

iDirectGov's 5G co-channel solution will mitigate interference for DIU mission partners, providing a critical capability to DOD users who experience 5G co-channel interference. This solution is built upon our CSIR technology, which delivers uninterrupted secure communications on any radio frequency to government users and allows them to thwart electronic warfare challenges.

As any signal interference is harmful to defense communications, our 5G co-channel capability will ensure our customers have the crucial interference mitigation tool that helps them with communications resiliency.

This initiative will open more communications avenues and improve interoperability across the military satellite sector.

We value partnerships with the DOD to bring innovations to the warfighter, enabling troops to meet mission success at the tactical edge. We look forward to continued work with the DOD to support clear lines of communication for critical *intelligence, surveillance and reconnaissance* (**ISR**), *communications on the move* (**COTM**), airborne and maritime communications in support of force protection, logistics, situational awareness, disaster recovery and emergency response.

We are hearing more about SATCOM interoperability. What are iDirectGov's thoughts on breaking down the barriers and bringing interoperability to reality?

TIM WINTER

In a perfect world, every SATCOM orbit and waveform would interoperate securely and effectively. This would provide users with options for their SATCOM and enable interoperable communications among various users and agencies, including with the DOD. Breaking down interoperability barriers means easier collaboration in times of disasters, emergencies and other events, as well as greater resiliency from provider outages, overloads, signal degradation, interference and signal loss.

Though interoperability is especially critical for MILSATCOM to ensure mission success, barriers such as technology, security and intellectual property secrets keep providers in the SATCOM ecosystem from sharing their proprietary information, which makes interoperability challenging.

How do we get there for interoperability to become a reality?

What is needed is a platform that seamlessly interoperates with various satellite services and waveforms. The key elements to this, as we see them, are virtualized waveforms and a platform that connects with various satellite services and waveforms. This is our idea to answer the interoperability challenge.

We believe that the best way to break down the obstacles and support interoperability is a ***Waveform Development Kit*** that streamlines the process of putting third-party waveforms on SDRs.

We consider our REVOLUTION 450mp SDR a real step forward for interoperability. The multi-waveform, multi-orbit SDR gives the DOD options for satellite orbits and waveforms, especially for mission-critical operations, including secure satellite communications and ISR. The man portable modem allows operators to build and run multi-orbital communications networks that can stand up to cyber and electronic warfare threats. However, this SDR technology alone isn't enough. We need modems that incorporate waveform virtualization and support third-party waveforms.

Our 450mp SDR, in conjunction with iDirectGov's Waveform Development Kit, enables iDirectGov and third-party waveforms to be virtualized and run on the 4-Series platform. Security is accomplished with intellectual property protection. Third parties using iDirectGov's Waveform Development Kit can provide an encrypted core to iDirectGov, thus protecting the intellectual property.

iDirect Government's ***4-Series*** suite of SDR modems, combined with the Waveform Development Kit, will provide maximum resilience, security, and SWaP for DOD customers while supporting commercial innovation and development by protecting IP with encryption and licensing options.

The ability of a single modem platform to react to the situation at hand provides massive flexibility and redundancy for users. These specialized satellite modems are the path forward for defense communications. By operating in multiple orbits and waveforms, interoperability can be achieved. Additionally, defense users can select the satellite service provider of choice for their critical communications and have redundancy in operations should there be an outage.

The company established the iDirectGov Engineering Center of Excellence, where iDirectGov's specialized engineers work on the most advanced, secure and resilient satellite ground systems and functionality. How is this paving the path forward in security for MILSATCOM?

TIM WINTER

Our ***Engineering Center of Excellence*** enables the company to better respond to ever-evolving EW and cyber threats and to meet defense and government requirements for faster-paced MILSATCOM innovation.

We've co-located the Center of Excellence with iDirect Government's existing engineering team. This ensures that the in-field experience of the firm's veterans contributes to building exceptional, high-performance products that withstand the most excruciating circumstances in the harshest of environments.

Coming out of the center are new SDR modems, defense platforms, and other military standard solutions. The center enables development of the most advanced features in our

product portfolio, particularly in building security-focused solutions that meet the rugged needs of the warfighter and maximum satellite communications.

The center and the engineering team solve some of the most complex challenges facing defense and government today, allowing us to quickly and effectively address new jamming, cyber and EW threats.

How essential are multi-orbit multi-waveform capabilities for mission-critical operations?

TIM WINTER

Defense and military customers fully expect and need flawless MILSATCOM when conducting missions. Multi-orbit, multi-waveform technology is the path to ensuring critical DOD communications.

By operating in multiple orbits and using multiple waveforms, defense users can select the satellite service provider of their choice and have redundancy in operations should there be a satellite communications outage. This is particularly important to support multi-mission capabilities for voice, data and video defense communications.

Multi-orbit/multi-constellation capability provides maximum communications spectrum potential with the least amount of risk for the military. And, as technologies always are advancing, multi-waveform is the future to satisfy the requirements of the MILSATCOM end-user.

Incorporating multiple waveforms in a single, compact modem required a new physical architecture to meet SWaP and industry requirements. SDRs that a multi-orbit, multi-waveform strategy; GEO, MEO, HEO and LEO orbits, and a variety of waveforms, meet those needs.

The future depends on implementing the best options for critical MILSATCOM to keep the homeland safe, and the best options include multi-orbit, multi-waveform connectivity.

You recently teamed with Tampa Microwave for the TerraNet mission readiness solution. How important is this partnership? How valuable are teaming arrangements in MILSATCOM?

TIM WINTER

We are thrilled to have ***Tampa Microwave*** as a satellite network partner. We combine iDirect Government's Tactical Hub and Tampa Microwave's ***Quad Band Satellite Simulator*** (**QBSS**) to deliver an easy-to-use, transportable and cost-effective solution to support all-encompassing mission-readiness scenarios, branded TerraNet.

This partnership offers a way to prepare for mission readiness and save on bandwidth costs. TerraNet can be used to perform end-to-end system validation, RF equipment testing, training, maintenance and pre-deployment exercises of hub and remote terminals in a simulated satellite network.

This is another example of how we are at the forefront of innovation. By combining forces with Tampa Microwave, we further increase the resilience, efficiency, flexibility and scalability of SATCOM for our customers.

Teaming arrangements are important to meet the DOD's emerging requirements and represent a means to advance capabilities. We will continue to leverage existing partnerships and forge new ones with SATCOM leaders. We will foster innovation and pool expert resources as we tackle complex engineering challenges. By building a collaborative ecosystem, we accelerate advancements and enhance the overall capabilities of our satellite solutions.

Collaboration brings about innovations to help our warfighters execute their missions, and we will continue to partner with industry to innovate, enhance customer satisfaction and success, and make SATCOM dynamic.

What is your personal outlook for MILSATCOM in 2025?

TIM WINTER

At iDirectGov, in 2025, we will continue to advance the security and reliability of military communications, delivering innovative solutions for combatting satellite interference and enabling improvements in the quality and integrity of satellite communications.

Security countermeasures will be engineered into every one of our Defense-based solutions. We will further elevate our electronic warfare efforts, helping to combat communication EW vulnerabilities with the integration of our CSIR countermeasure application into new solutions and services. Additionally, we will incorporate the latest military standards into our products and services.

This will enable MILSATCOM to operate despite bad actors who try to interfere with critical communications used for command and control, intelligence, situational awareness, logistics and other military needs.

Emerging technologies will continue driving innovation in 2025, notably 5G connectivity, *artificial intelligence and machine learning* (**AI/ML**).

Resiliency and security remain necessary for all next-gen networks, platforms and ecosystems.

There's been much talk about artificial intelligence (AI) and its benefits to all industries. In SATCOM, we'll see AI enabling greater automation and even dynamic bandwidth allocation and demand-based satellite network access.

AI can be used to assist in the determination of a jamming and in interference evolution.

Advance technology integration is critical to stay ahead of malicious actors and keep our troops safe. Our adversaries will look to implement AI as a weapon on the battlefield. We will be developing new technologies to counter these efforts, using AI to fight the fight. AI-powered solutions will be developed to confront enemies and bad actors.

We will continue to drive innovation in the coming new year and meet our customers' needs and challenges. My vision is to develop secure global connectivity that has no limitations on land, at sea and in the air. We can do this by hardening MILSATCOM and enabling resiliency.

This will enable MILSATCOM to operate despite bad actors who try to interfere with critical communications used for command and control, intelligence, situational awareness, logistics and other military needs.

What technologies do you believe will come to the forefront in 2025?

TIM WINTER

We will see more advanced technology integration in the entire SATCOM ecosystem, including 5G connectivity, AI and machine learning, as well as anti-jam advances, cyber security modernizations and the pioneering applications of new technologies.

2025 will be a year that we witness multi-orbit and multi-waveform capabilities taking shape. Integration and interoperability in the ground segment will start to take center stage in providing open architecture attributes, allowing the warfighter to access various SATCOM network solutions.

These multi-orbit, dynamic capabilities will support advanced mobility requirements and revolutionary operational efficiencies for the warfighter, first responders, disaster recovery personnel and field operators.

Given your work within the U.S. Navy, the commercial SATCOM world and now the MILSATCOM environs, when you review your career to date, what projects truly bring a sense of satisfaction to you?

TIM WINTER

I have enjoyed my work at every stage of my journey. All projects have provided different opportunities and challenges. True satisfaction in each instance, however, was borne out of the people I worked with. Seeing the team or organization succeed was paramount in everything I have done.

I think these experiences have greatly influenced my approach to a servant style leadership and a true foundational belief that we all must be part of something bigger than ourselves to truly enjoy fulfillment and satisfaction.

As we round out 2024, the next year holds great promise for MILSATCOM advancements that will benefit the warfighter.

www.idirectgov.com

MULTI-ORBIT SATCOM

BOOSTING U.S. ARMY NETWORK RESILIENCY CAPABILITIES IN LARGE SCALE COMBAT OPERATIONS

Author: Amy Walker, Project Manager Tactical Network, PEO C3T Public Affairs

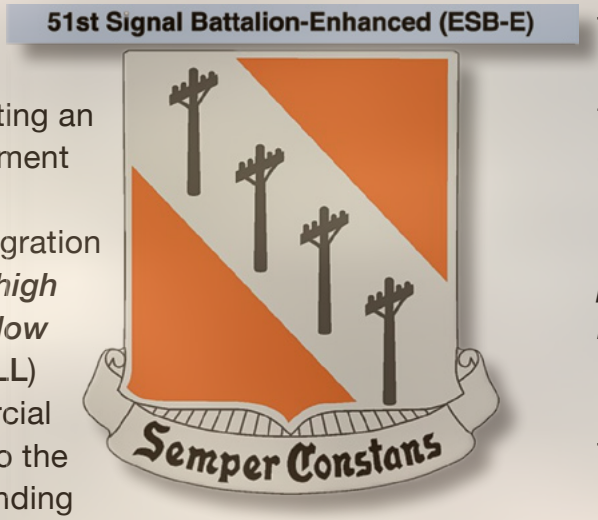
*Headquartered at Aberdeen Proving Ground, Maryland, the Program Executive Office for Command, Control and Communications-Tactical (**PEO C3T**) is responsible for delivering a unified network that addresses the most critical operational needs and supports the Army of 2030.*

The Army is leveraging satellite capabilities in multiple Earth orbits to deliver the network throughput, low latency, and resiliency it needs for future operations.

For several years, the Army has been working closely with commercial vendors through streamlined ***cooperative research and development agreements***, known as **CRADAs**, to securely integrate and explore the capabilities of emerging commercial ***Low Earth Orbit*** (**LEO**) and ***Medium Earth Orbit*** (**MEO**) satellite constellations, as well as the services and ground terminals needed to access them.

Now that some of these commercial solutions are maturing and expanding in global coverage, the Army has begun to conduct operational assessments to inform near- and long-term network design decisions.

"*With the added multi-orbit capabilities, our communications pathways are more diverse, robust, and present a greater challenge for an adversary to overcome*," said ***Lt. Col. Nicolas Beck, commander of the 51st Expeditionary Signal Battalion-Enhanced (ESB-E), 22nd Corps Signal Brigade***.



The **51st ESB-E** has been supporting an Army assessment to inform the potential integration of emerging ***high throughput, low latency*** (**HT/LL**) LEO commercial **SATCOM** into the Army's expanding **Unified Network** transport arsenal.

Recent geopolitical conflicts continue to underscore the need for commanders to possess multiple transport options to enhance their ***primary, alternate, contingency, emergency*** (**PACE**) communication plans to ensure resilient rapid uninterrupted data exchange on the battlefield. The more agnostic transport network pathway options that exist for data to travel through — especially in disrupted, ***disconnected, intermittent and low-bandwidth*** (**DDIL**) environments--the more resilient the network becomes to signal roadblocks, including enemy jamming.

"*A strong PACE plan will be critical to any future large scale combat operation*," Beck said. "*Previous SATCOM equipment was limited to only connecting to satellites in Geosynchronous Earth Orbit [GEO]. This is a single transport option that the high throughput, low latency capabilities eliminate by giving us access to MEO and LEO satellites*."

Additionally, HT/LL capabilities help reduce military signature, enabling the Army to blend its electronic signature with existing commercial signatures within the area of operation.

This presents a challenge to adversaries, making it harder to identify which SATCOM links to jam, causing them to spend more time and resources identifying dispersed command post locations, Beck said.

"*In short, the high throughput, low latency capabilities provide commanders with more bandwidth, a reduced military signature, and longer survivability*," Beck said.

THE ASSESSMENT

The HT/LL assessment supported by the 51st ESB-E leverages several different maturing commercial LEO solutions integrated with the unit's organic baseband systems. The purpose is to determine the best mix of solutions to potentially add HT/LL transport to the Army's portfolio of SATCOM terminals. The assessment will also inform ***concept of operations*** (**CONOPS**) and ***tactics, techniques and procedures*** (**TTPs**) for future HT/LL use in Army units.

The unit will deploy and use the commercial assets in a variety of training exercises, mission sets and locations, said ***Col. Stuart McMillan, project manager for Tactical Network (PM TN), at the Program Executive Office Command, Control, Communications-Tactical (PEO C3T)***, which is managing the HT/LL Assessment for the Army.

"*The valuable quantitative and qualitative data points and Soldier feedback we collect from the assessment will help shape Army high throughput, low latency requirements and drive future decisions on what to procure and how to implement materiel solutions to meet those requirements*," McMillan said.

The PM fielded the ***Scalable Network Node*** (**SNN**) antenna and baseband, to the 51st ESB-E as part of the unit's conversion from an ESB to an ESB-E formation, in April of 2023.

Then to support the HT/LL Assessment, the project office facilitated the training on the commercial HT/LL solutions in September of 2023, at the unit's home station at _____ (**JBLM**) in Washington.

PM TN will also conduct a HT/LL MEO Assessment leveraging ***Scalable Class Of Unified Terminal*** (**SCOUT**)-***Medium*** satellite terminals, to evaluate whether MEO SATCOM could be a viable solution for transport diversity at division and above headquarters, McMillan said.

SCOUT-Small (0.65m/0.95m):

- *Transportable in three hard side transit cases*
- *Supports 12 users over multiple enclaves*
- *Airline checkable for commercial transport*
- *Rapidly setup by two Soldiers*
- *Tri-band capable (X, Ku, & Ka)*

SUPPORTING NETWORK MODERNIZATION

Two of the main benefits drawing the Army to integrate LEO and MEO network transport communication capabilities into the network design are the huge increase in bandwidth and reduction in latency they provide, compared to current GEO capabilities.

"*If you can imagine a signal transmitted from a ground satellite terminal traveling at the speed of light, it would connect with the LEO satellites first, over current GEO satellites, due to the shorter distance*," said ***Warrant Officer 01 (WO1), David Hernandez, network technician for the 51st ESB-E.*** "*This cuts down on data round trip times, and drastically improves the latency, giving ground commanders a better command and control (C2) experience*."

Commercial LEO and MEO SATCOM significantly improve the performance of the network and the Army's mission command systems, especially for real-time applications that provide the resilient data exchange commanders need to understand the battlefield and make rapid informed decisions.
As the Army continues to move toward a more data-centric operational environment, its need for HT/LL capabilities increases, as more data is stored in the cloud. HT/LL multi-orbit SATCOM capabilities, along with ***automatic*** (**Auto**) PACE communications, are foundational elements for *tactical edge cloud computing*, *distributed C2*, *on-the-move* network connectivity.

AUTOMATING PACE

In support of the HT/LL SNN Assessment, PM TN installed an Army Auto-PACE software capability, known as ***Seeker***, to help facilitate the use of commercial LEO links. Seeker increases bandwidth through aggregation, quick detection of link outages and rapid, automated self-healing.

Adaptive network connections determine the optimal signal path at any given moment to enable rapid and reliable data transfer. The automated changeover to different PACE options is seamless to the end user and reduces network complexity at the edge, so Soldiers can focus on the fight.

"*Seeker is a multifaceted software in that it can merge multiple forms of transport, such as satellite, Troposcatter, TRILOS, cellular, etc. into one stream to improve bandwidth and throughput capabilities for the warfighter and other customers*," Hernandez said. "*It also has a bleed over feature in which one transport method can be capped at a certain bandwidth with the excess data bleeding over into another transport. In either case, it serves our customers an enhanced network experience*."

As commercial LEO and MEO satellite capabilities, as well as protected high capacity GEO military capabilities, continue to mature and expand globally, the Army is carefully laying a strong foundation to enable the secure integration of the right transport agnostic, multi-band, muti-orbit solutions, and combination of solutions, into its Unified Network design, at the right time and cost.

"*Auto-PACE and high throughput, low latency multi-orbit SATCOM capabilities are essential to the Army's network modernization efforts*," Beck said. "*Army data requirements continue to grow, and both technologies enable maximum data throughput, while ensuring a reliable network for commanders to communicate*."

PEO C3T

The U.S. Army Program Executive Office Command, Control and Communications-Tactical (PEO C3T) develops, acquires, fields and supports the Army's Unified Network to ensure force readiness in both current missions and potential future large scale combat operations. This critical Army modernization priority delivers resilient terrestrial and satellite communications capabilities to ensure commanders and Soldiers remain connected and informed at all times, even in the most austere and hostile environments. PEO C3T is delivering an integrated Unified Network to regions around the globe, enabling high-speed, high-capacity voice, data and video communications to an Army user base that includes joint, coalition and other mission partners.

DISPATCHES

SpacePath's high performance uplink amplifiers cover all mission-critical segments including high-throughput satellite (HTS), mobile satellite, fixed-Earth stations and MILSATCOM.

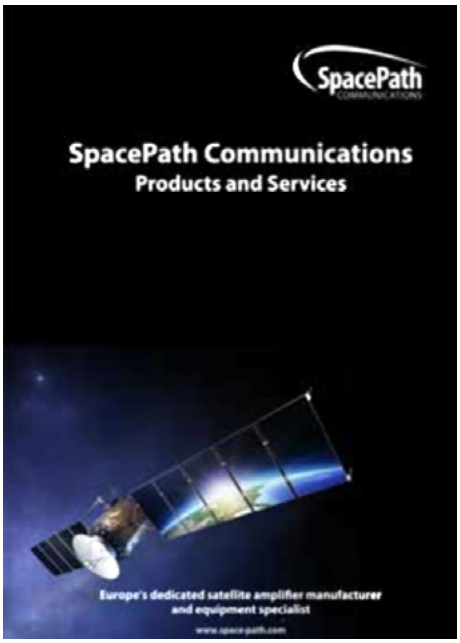
Colin Bolton, director of business development, SpacePath Communications, said, *"This new development reinforces SpacePath's position as a supplier of choice for mission-critical connectivity. Leveraging our design expertise, we have broadened our portfolio in troposcatter systems to include a military-grade, microwave terminal for communications beyond the horizon while on the move."*

SpacePath intros military grade man-pack terminal for troposcatter comms

SpacePath Communications is going to be showcasing their new 40W man-pack terminal for tropospheric scatter (troposcatter) transmission at the Defence in Space Conference (DISC), London.

The military-grade, troposcatter man-pack highlights a cutting-edge solution in the Beyond Line-of-Sight (BLoS) communication segment, combining a BUC, LNB, modem and filters in a single, lightweight, and ruggedized, portable terminal. Offering up to 20W of linear output power and a frequency range of 4.4-5.0GHz, this compact device provides exceptional power density, and weighs less than 6 kg. The robust man-pack is designed for long-range, point-to-point communication, ideal for tactical military operations, disaster recovery, and emergency restoration, ensuring reliable communications in locations where traditional SATCOM is unavailable.

Providing exceptional flexibility in deployment, the terminal is compatible with all antenna systems and supports data rates of at least 7 Mbps over distances of up to 70km. The integrated modem with quad-diversity further enhances performance, making it ideal for demanding, tactical communications.



Download the SpacePath Communications product brochure

RTX's Raytheon + Northrop Grumman successfully test solid rocket motor

__ _____, an RTX (NYSE: RTX) business, and _____ __ _____ (NYSE: NOC) have successfully completed a static fire test of an advanced, long-range, solid rocket motor at the Northrop Grumman Allegany Ballistics Laboratory in West Virginia.

The test demonstrated wired, end-burning technology for hypersonic applications and provided data to support digital modeling and simulations that validated the design maturity and performance of the rocket motor. Raytheon's **Advanced Technology** team and Northrop Grumman leveraged their combined digital engineering expertise to accelerate the design and development in a digital environment using model-based systems engineering.

Raytheon and Northrop Grumman share a long history of collaborating on the development of hypersonic systems. Both are making investments in rocket motor testing to prove design stability and maturity that is necessary to deliver capability to servicemen and women on an accelerated schedule.

"This is a major milestone in proving the significant capability of this solid rocket motor," said ***Colin Whelan, president of Advanced Technology at Raytheon****.*
"By leveraging industry collaboration, we were able to demonstrate that we can produce and meet requirements for challenging long-range fires kill chains."

"This extremely important test of our wired end-burning technology provides extended range over conventional rocket motors," said ***Frank DeMauro, vice president, Weapon Systems, Northrop Grumman****. "We are excited to rapidly push the boundaries on next-generation propulsion technology and provide our customers with the ability to respond to evolving threats."*

SATCOM providers changing tactics to compete with NGSO-led capacity growth

_____ ____ has released its latest edition of the 'Satellite Connectivity & Video Market' report, revealing significant shifts across the SATCOM industry.

The past three years have seen a dramatic, eight fold increase in global satellite capacity supply, reaching around 27 Tbps in 2023, a figure that is accounted for more than 80% by Starlink. This dominance can be partially attributed to delays from initial target dates from most other constellation projects and software-defined satellites. However, new LEO constellations, such as **Telesat**, **Lightspeed**, and **Amazon Kuiper**, alongside second-generation **Starlink** and ***Eutelsat OneWeb*** constellations, as well as *Very High Throughput Satellites* (**VHTS**) such as ***Viasat-3***, are expected to drive growth to 260 Tbps by 2029.

The rise of ***Non-Geostationary Satellite Orbit*** (**NGSO**) systems has caused a decline in orders for GEO satellites, as operators have adopted a "*wait and see"* approach. Despite this, GEO capacity still represented approximately 85% of capacity revenues in 2023, though NGSO capacity revenues are projected to grow at a *Compound Annual Growth Rate* (**CAGR**) of 27%, surpassing GEO revenues by 2028 and bringing in around $18 billion by 2033.

GEO-High Throughput Satellite (**GEO-HTS**) systems continue to maintain significant traction in premium market segments, such as MILSATCOM, aeronautical connectivity, and certain areas of fixed broadband, particularly those requiring high uptime or ***Committed Information Rate*** (**CIR**)-based ***Service Level Agreements*** (**SLAs**). However, Starlink accounted for 70% of total HTS traffic in 2023, intensifying competition in key markets like consumer broadband and maritime, further challenging traditional GEO players in these segments.

In response to rising competition, satellite operators are also pursuing vertical and horizontal integration strategies. This includes two significant closed merger and acquisition deals in 2023 – **Viasat**'s acquisition of **Inmarsat** and **Eutelsat**'s merger with **OneWeb** – as well **SES** announcing it was acquiring **Intelsat** in 2024, with regulatory clearances expected to be received in 2025.

Consequently, the rising competition should contribute to the ***Average Revenue Per Unit*** (**ARPU**) for satellite capacity falling below $100 per Mbps per month across most segments by 2033. This price decline is set to unlock new opportunities in rural, remote, and under-connected areas, including those near urban centers and over oceans, driving global capacity demand to 73 Tbps by 2033 (27% CAGR).

The industry's total service revenues are thus projected to reach approximately $117 billion by 2033, capturing the expanding addressable market. However, the anticipated return to growth in service revenues may be delayed due to a continued rapid decline of the video segment in mature digital markets and a stagnation in previously growing emerging markets, such as South Asia. Additionally, delays in the deployment of NGSO constellations and VHTS capacity have also slowed service revenue growth in key data segments such as Enterprise Networks.

> *"Facing a shifting landscape marked by declining demand for video broadcasting, fluctuating mobility market patterns, and an influx of capacity from NGSO constellations, satcom operators have been exploring different strategies to survive," said* ***Dimitri Buchs, Manager at Novaspace and lead author of the 'Satellite Connectivity & Video Market' report****. "In order to expand market reach, diversify service offerings, and enhance business resilience, capacity providers have been increasingly forming 'multi-orbit' partnerships.."*

Boeing developing quantum comms tech with in-space test satellite

[NYSE: BA] has scheduled a 2026 launch of a satellite – dubbed Q4S – which is designed to demo quantum entanglement swapping capabilities on-orbit — this Boeing-funded, first-of-its-kind space mission brings humanity closer to building a secure, global quantum internet that connects quantum sensors and computers.

Quantum sensors are much more precise than today's state-of-the-art instruments and quantum computers have the capacity to process large amounts of data, offering potential to revolutionize an array of industries. This experiment is attempting to demonstrate quantum networking in space, helping to better understand how these networks can be built across vast distances and remain highly synchronized.

Boeing is setting the stage for a revolution in how the company handles information with secure, quantum-enhanced applications, such as fault-tolerant systems that reduce errors in computing, secure voting mechanisms that protect electoral integrity, and blind quantum computing which allows data to be processed without exposure.

Entanglement swapping relies on quantum teleportation – a method where the information carried by a particle can be transferred without having to move the particle itself across the distance. ***Albert Einstein*** famously referred to this ethereal concept as "*spooky action at a distance*," underscoring the complex nature of quantum mechanics.

Quantum networking capabilities in space can unlock new potential, helping researchers gather more data about the Earth and space environments – areas where current instrument sensitivity and resolution limit progress.

The year-long Q4S demonstration involves two entangled-photon pair sources housed within a space vehicle. Boeing's payload and technology partner, HRL Laboratories, a joint venture between Boeing and GM [NYSE: GM], has made significant advancements in benchtop exercises as the joint team finalizes technical designs of a space-hardened payload that is ready for launch.

*"We're making a big bet on quantum technology," said **Jay Lowell, chief engineer for Boeing's Disruptive Computing, Networks & Sensors organization**. "Quantum entanglement swapping underpins the communication of the future, expanding quantum networks beyond simple point-to-point communication. We're launching Q4S to prove it can be done on-orbit. By demonstrating entanglement swapping, we can create a scalable network, where quantum information can be transmitted over vast distances, something currently limited by decoherence and loss."*

*"Boeing has always served as a pioneer, pushing the boundaries of what's possible," said **Todd Citron, Boeing's Chief Technology Officer.** "We're doing much more than participating in quantum research, we are leading the way to operationalize and scale quantum technologies for global applications."*

Orbit secured million$ advanced SATCOM contract for Asian naval military platforms

Orbit Communication Systems Ltd. received a $6 million contract late last month with a prominent Asian integrator to supply advanced satellite communication (SATCOM) systems for new naval military platforms.

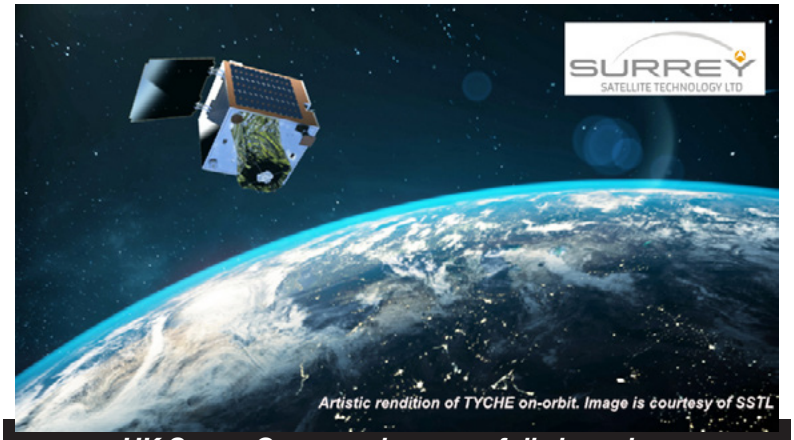
These _____MIL systems will be delivered between 2025 and 2030, providing continuous satellite connectivity across multiple frequencies for a leading global fleet.

The OceanTRx 7MIL is the latest addition to a long line of more than 30 years' field proven maritime SATCOM terminal systems with leading NATO and allied navies. It provides reliable, high capacity, long-range communications to navy vessels in extreme conditions. This satellite communication system supports a variety of antenna system configurations.

With a diameter of 2.2 meters, the OceanTRx 7MIL operates on X, Ku, Ka and C frequencies, and enables simultaneous operation of a variety of frequencies for global activities. The OceanTRx 7MIL can be connected to a unique Orbit switching matrix (OSM) which allows multiple internal connections and switching of up to 8 antennas and 8 modems according to customers' requirements.

The OceanTRx 7MIL is designed to operate in the crowded and hostile EMC environment of a modern warship, and has minimal impact on other communication, sensor and weapon systems. Designed for quick and convenient installation, maintenance and upgrade, the system provides defense customers with a combination of exceptional RF performance and availability.

Daniel Ashchar, CEO of Orbit, said, "This order represents another significant milestone in expanding our order backlog this year. We are proud to continue our partnership with a leading Asian integrator, delivering Orbit's cutting-edge systems for a prominent global fleet. The OceanTRx 7Mil platform underscores our leadership in military marine communication solutions, offering a dual-band capability that meets both military and civilian needs on a single system. We are committed to building a significant backlog to support our ongoing growth as a leading company in our field."



UK Space Command successfully launches first military satellite

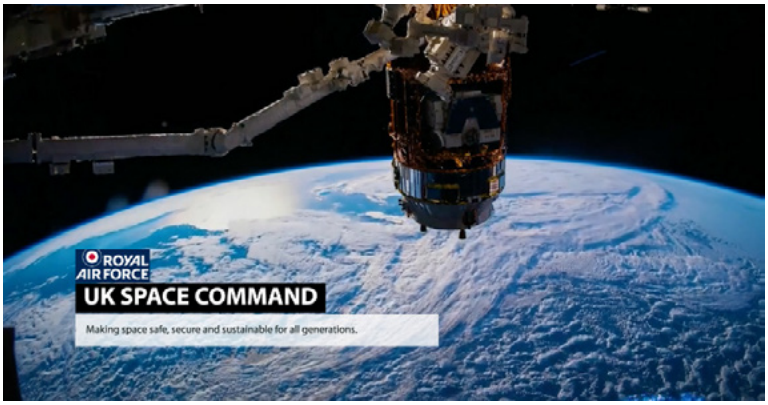
A UK satellite to support military operations has been successfully launched. Named* Tyche*, the satellite is ____ _____'s first satellite which can capture daytime images and videos of the Earth's surface. The satellite will strengthen the UK's Intelligence, Surveillance, and Reconnaissance (ISR) capabilities.

As the conflict in Ukraine has shown, the use of space is crucial to military operations. Tyche is the first satellite to be launched under the UK Ministry of Defence's space-based ISR program, which will deliver a constellation of satellites and supporting ground systems by 2031.

These satellites will support military operations as well as contribute to other government tasks, including natural disaster monitoring, the development of mapping information, environmental monitoring and tracking the impact of climate change around the world.

Designed and built in the UK through a £22 million contract awarded by Defence Equipment & Support to ____ _____ _____ (**SSTL**), Tyche is the first satellite to be fully owned by the Ministry of Defence.

SSTL received the first signals from Tyche – which is comparable in size to a washing machine – a few hours after lift-off, confirming the successful launch. Operating in LEO over a five-year lifespan, Tyche will provide timely space-based imagery in support of the UK Armed Forces. The design and build of the 150-kilogram satellite has supported around 100 high-skilled roles at SSTL since 2022.

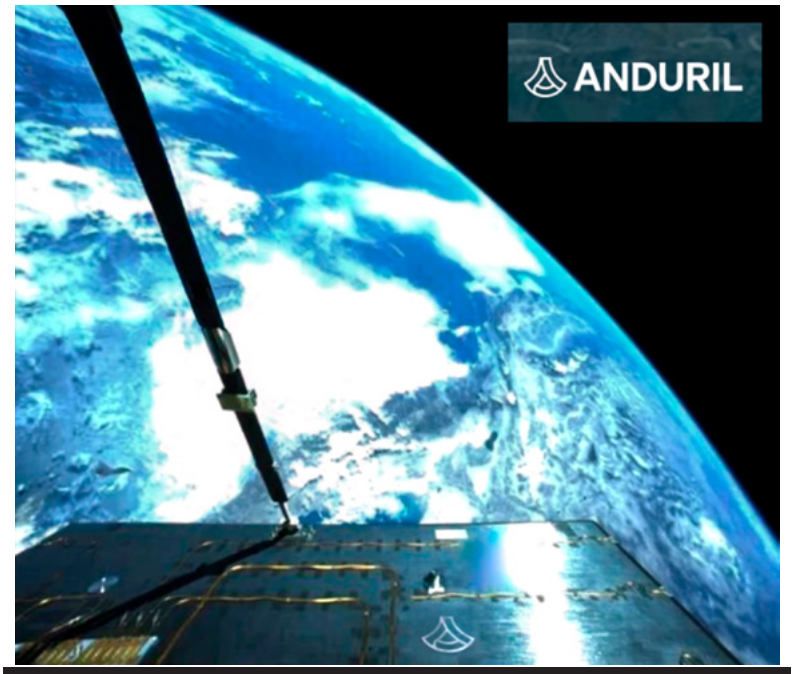


Tyche was launched from **Vandenberg Space Force Base**, California, by SpaceX, on their re-usable Falcon 9 rocket, as part of the **Transporter 11** mission.

Minister for Defence Procurement and Industry, Maria Eagle, said. "Tyche will provide essential intelligence for military operations as well as supporting wider tasks across government. Tyche also shows the UK's commitment to support innovation in science and technology, stimulating growth across the sector and supporting highly skilled jobs in the UK."

UK Space Commander, Major General Paul Tedman, said, "This is a fabulous day for UK space. The successful launch of Tyche has shown that UK Space Command, and its essential partners across defence and industry, can rapidly take a concept through to the delivery of a satellite capability on orbit. Tyche represents the first of a future constellation of Intelligence, Surveillance, and Reconnaissance satellites that we'll launch over the coming years. I'd like to take this opportunity to congratulate everybody involved with Tyche and thank them for their support."

Paul Russell, DE&S Space Team Leader, said, "Working closely with UK Space Command, Dstl and industry to understand how to deliver in a new, complex and critical environment has been an exciting journey. To see Tyche – the first of a new generation of UK military capabilities – delivered into orbit is an incredibly proud moment and a tribute to everyone's commitment to this key project."



Anduril is expanding into the space domain to enhance mission-critical ops for warfighters

_____ is expanding their advanced, AI-powered hardware and software capabilities into the final frontier: Space. This effort will enhance mission-critical Space Domain Awareness (SDA), Space Control, and Command and Control (C2) for U.S. military warfighters and allied partners, providing end-to-end solutions to address the growing threats posed by adversaries in space.

The firm's goal is to develop fully integrated hardware and software systems, using _____ _____, modular mission payloads, and strategic partnerships across the space industry. Space is a contested warfighting domain and we recognize the importance of equipping spacecraft with advanced autonomy and cutting-edge payloads, ensuring the nation's Guardians maintain a decisive advantage in every mission.

With multiple hardware and software payloads already deployed on-orbit, we are not waiting. Anduril is investing the company's own internal dollars to mature the firm's capabilities for the space domain. Anduril is rapidly delivering advanced systems that range from on-orbit edge processing of sensor data to resilient satellite command and control. These advancements build upon the company's work with Space Systems Command to enhance communications within the Space Surveillance Network, by now working to advance the state of the art in linking ground-based sensors and space-based assets for better awareness of orbital threats. Anduril is extending the software platform, Lattice, to autonomously monitor and manage space-based assets, improving situational awareness and reducing operator workload.

The platform's proven capabilities in air, land, and sea operations will now be extended to the space domain, integrating with spacecraft, payloads, and software built across the industrial base. Anduril will design, manufacture, and integrate modular mission payloads designed to enable unique mission requirements, leveraging our extensive expertise across imaging, electronic warfare, command and control, and mission autonomy.

These payloads will provide warfighters with real-time data exploitation, autonomous coordination of satellites, and resilient communication capabilities. Anduril's focus on modularity and adaptability ensures that these solutions can evolve alongside the rapidly changing threats across a variety of different orbits.

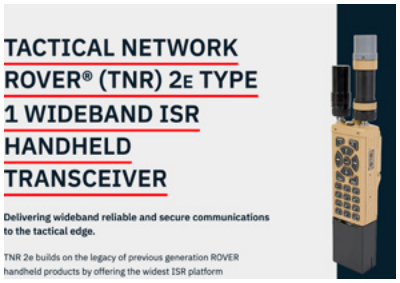
Anduril is investing their own IRAD to design, build, and launch our own fully integrated systems by the end of 2025. This mission will serve as a testbed for maturation of multiple Anduril and third party payloads which we will be announcing in the coming months. By launching and flying systems frequently, we can ensure that lessons are quickly learned and incorporated ahead of critical customer operations.

Anduril is dedicated to fostering partnerships across the space industry to ensure the most advanced solutions are delivered to the warfighter and believes that an open and collaborative approach within the U.S. industrial base is essential to compete with adversaries making significant investments in this domain. In the coming months, the company will announce upcoming partnerships with satellite hardware suppliers, launch service providers, and ground system developers that will drive the development of best-in-class solutions on behalf of the government.

DISPATCHES

L3Harris receives a million$$$ IDIQ from the U.S.A.F. for video data link

_____ ***(NYSE:LHX) has received an Indefinite Delivery, Indefinite Quantity (IDIQ) contract worth up to $182 million from the U.S. Air Force to deliver advanced situational awareness capabilities.***



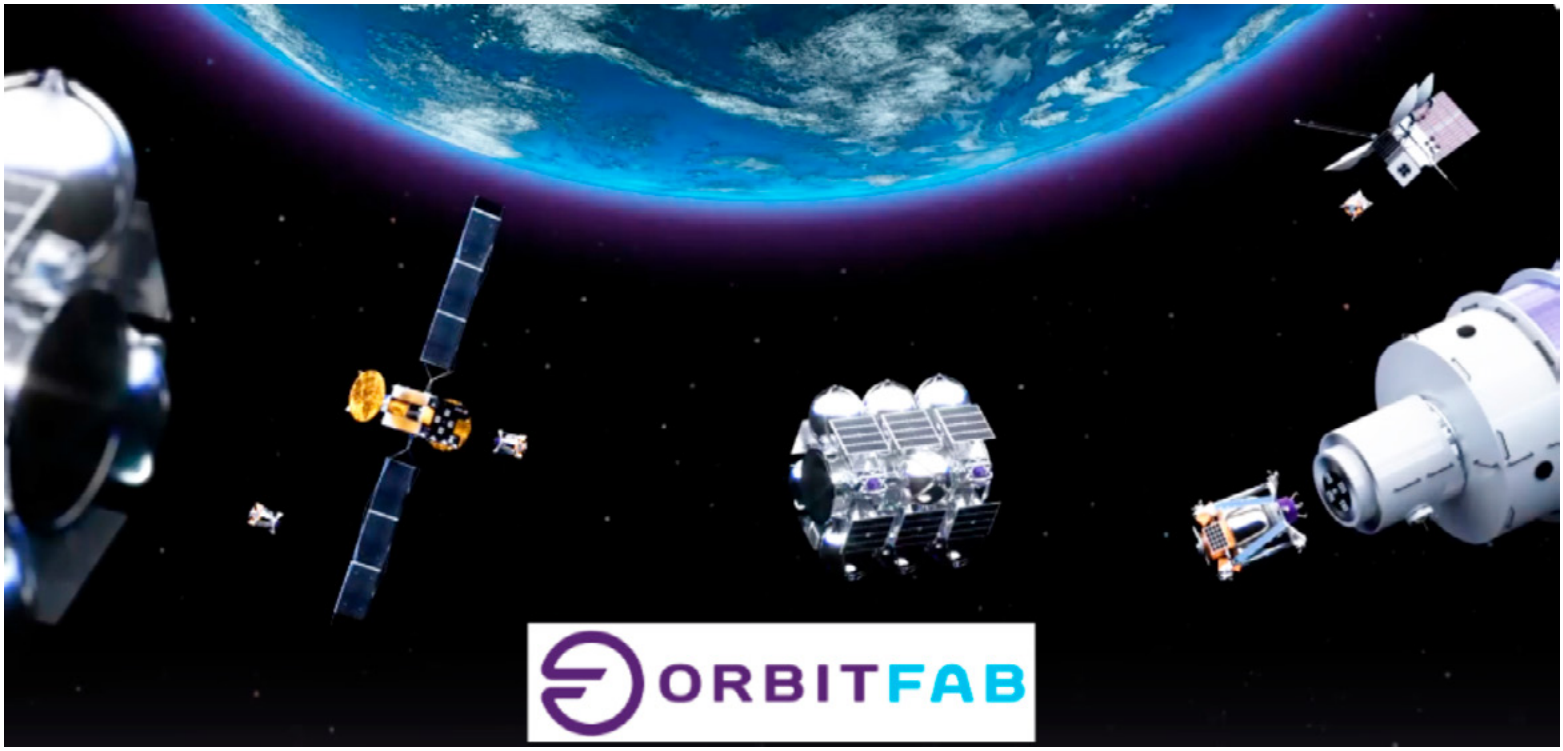
Partnering with the _____ _____ _____, this contract will enable L3Harris to provide economies of scale for the U.S. Department of Defense and allied nations when procuring critical ***Video Data Link*** (**VDL**) technology, including the _____ ___ and _____ wideband ISR handheld transceivers.

Designed for air, surface and maritime use, the ROVER 6S provides real-time, ***full-motion video*** (**FMV**) and other data for situational awareness, surveillance, convey overwatch operations and other situations where eyes-on-target are required. The TNR 2 handheld transceiver provides a multi-megabit, bi-directional data link capability to the most disadvantaged users – dismounted ground combat troops.

This award is the third consecutive, five-year VDL IDIQ L3Harris has received under the program. Delivery of vital data access through the VDL III program furthers the company's support of customers' Combined Joint All-Domain Command-and-Control requirements, which also includes membership in the _____, continued success in the Air Force Research Laboratory's ***Defense Experimentation Using Commercial Space Internet*** program and ongoing production on resilient communications' devices and systems for the U.S. Army, Marine Corps and allies around the world.

As a member of the Advanced Battle Management Systems Digital Infrastructure Consortium, L3Harris will help define capabilities to enable the Department of the Air Force's vision for Joint All-Domain Command and Control.

"Coordinating with the Air Force as partners to leverage existing tools and authorities drives greater value for domestic and international customers on an exponential scale," said Lauren Barnes, President, Broadband Communications Systems, L3Harris. "The collaboration allows the Air Force to work directly with numerous organizations modernizing their video data link capabilities to determine schedules that best meet their needs and coalition forces as a whole."



USSF approves Orbit Fab's RAFTI as accepted refueling interface for military satellites

_____ has announced that the firm's _____™ (Rapidly Attachable Fluid Transfer Interface) refueling port has been designated by the _____ _____ _____ _____ _____ _____ as a refueling interface for in-space fueling of military satellites.

The SSC's System Engineering Review Board (SERB) made the recommendation following mission-critical assessments that RAFTI meets the technical qualifications to support a wide range of U.S. Government space missions.

Orbit Fab is well positioned with its RAFTI refueling port and GRIP™ refueling nozzle to meet the Space Force's request and need for refueling as a commercial service. In-space fuel depots equipped with RAFTIs, and fuel shuttles equipped with the GRIP will enable reusable fuel shuttles and satellites.

The Space Force Tetra-5 program satellites are set to be among the first to use Orbit Fab's RAFTI refueling ports during a first-of-its-kind refueling operations, expecting to launch next year. That's just one of many named and yet-to-be named government and commercial programs that have purchased RAFTI for spacecraft ground and on-orbit fueling capabilities. The DoD's _____ (**DIU**) has contracted with Orbit Fab for the first in-space fuel sale in GEO orbit and selected Orbit Fab as part of its RAPIDS Refueling and Fuel Depot Initiative.

Built as a small, affordable, commercially available refueling interface, Orbit Fab's RAFTI refueling port is ready for launch site fueling and in-space refueling of satellites of any size in any orbit, including the biggest national security, civil, and commercial spacecraft.

Orbit Fab's RAFTI is the first refueling interface to be flight qualified, a milestone reached earlier this year after completing a battery of stringent tests and rigorous evaluations. The RAFTI refueling port can be easily combined with the RAFTI ***Ground Coupling***™, a ground infrastructure interface that enables spacecraft operators, manufacturers, and payload processing facilities to replace typical fill-and-drain service valves with RAFTI for secure and reliable ground fueling at the launch site as well as in-space refueling.